

## Banking safely online

Online banking is an easy and convenient way to manage your money, and recently overtook telephone banking as our favourite method of remote banking.



It is also a very safe and secure way to access your bank account. Your chances of becoming a victim of online banking fraud are very low and banks are committed to keeping it this way.

However, because the banks' own systems have proved difficult to attack,

criminals have turned their attention to getting information directly from online banking customers themselves.

Nevertheless, by being vigilant and following simple safety procedures, you can significantly limit your chances of falling victim to online banking fraud.

## Common online banking scams

**Phishing** is the name given to emails that claim to be from your bank or other organisations but are actually sent to you by fraudsters. These emails typically urge you to click on a link that takes you to a fake website identical to the one you would expect to see. You are then asked to verify or update your personal security information but, by doing so, you are actually giving your information to the fraudster who has created the fake website. The fraudster then uses the details to access your online bank account and take your money.

One easy way to spot phishing emails is that they are usually addressed to "Dear valued customer" instead of using your name. This is because phishing emails are usually sent out at random as the fraudsters only have very limited information such as your email address.

Phishing incidents are usually targeted against banks and building societies. However, criminals will try other ways to get hold of personal information and emails of this nature are increasingly being sent out by fraudsters in the guise of other organizations – such as PayPal, Amazon, HM Revenue & Customs and Facebook.

**Spyware** is a type of computer virus that can be installed on your computer without your knowledge. It is capable of monitoring your PC activity, enabling fraudsters to capture your passwords and other personal information. To make

sure you don't become a victim of spyware, make sure you have up-to-date anti-virus and anti-spyware software installed. Seek technical support as soon as possible if your computer starts acting oddly.

**Money mules** are people who transfer money that has been fraudulently obtained, usually as a result of phishing scams, from one country to another. As most of the fraudsters behind phishing scams are located overseas, and it is not possible to make cross-border transfers out of UK online bank accounts, a money mule or money transfer agent is required to launder the funds.

Money mules are often innocent people duped into helping criminals transfer the fraudulently obtained money out of the country. Criminals offer prospective victims the chance to earn some easy money for a few hours work each week, usually just requiring that you have access to the internet. The fraudsters try to conceal the fact that the work is illegal by giving the position a job title such as 'UK representative', 'shipping manager' or 'sales manager'.

After being recruited by the fraudsters, money mules receive fraudulently-obtained funds into their online bank accounts. They then withdraw the money and send it to a fraudster overseas using a wire transfer service, minus a commission payment that they keep for themselves.

# Avoid online scams

Most fraud on online bank accounts involves a customer being duped into giving away their passwords and security information via a phishing scam, or through their PC being infected with spyware designed to steal the information. To help minimise your chances of being a victim follow these common sense precautions:

## Before you bank online

- Make sure your computer has up-to-date anti-virus software and a firewall installed.
- Install anti-spyware software on your machine.
- Download (from the internet) the latest security updates, known as patches, for your browser and your operating system. Set your computer to automatically download these updates if possible.
- Ensure your browser is set at its highest level of security notification and monitoring. The safety options are not always activated by default when you install your computer.
- Keep your passwords and PINs a secret – do not write them down or tell anyone what they are.

## While banking online

- Be wary of unsolicited emails or phone calls asking you to disclose any personal details or passwords. Your



bank or the police would never contact you to ask you to disclose your PIN or your online banking password.

- Always access your internet banking site by typing the bank's address into your web browser.
- Never go to a website from a link in an email and then enter personal details.

Whilst most people seem to be heeding the warnings about phishing attempts, some users are occasionally trying to hit back at fraudsters by replying to phishing emails and either deliberately providing bogus

information or letting the sender know that they are aware it is a scam. However, you should not reply - by doing so you could be putting your PC at risk of attack from malicious spyware.

- The login pages of bank websites are secured through an encryption process, so ensure that there is a locked padlock or unbroken key in your browser window when accessing your bank site. The beginning of the bank's internet address will change from 'http' to 'https' when a secure connection is made.
- Don't be conned by convincing emails offering you the chance to make easy money. If an offer looks too good to be true, it probably is.
- Never leave your computer unattended when logged in to your online account.

## When you have finished banking online

- Ensure you log off from your online bank account before you shut down, especially if you are accessing your online bank account from a public computer or at an internet café.
- Check your bank statements regularly and thoroughly. If you notice anything irregular on your account contact your bank as soon as possible.

Further advice and information is available at [www.banksafeonline.org.uk](http://www.banksafeonline.org.uk)

## What to do if you are targeted

### If you receive a phishing email

Your bank will never send you emails asking you to disclose PINs, login details or complete passwords – if you receive an email of this nature you should delete it. Phishing emails can be reported to the banking industry by visiting [www.banksafeonline.org.uk](http://www.banksafeonline.org.uk) and clicking on 'Report a scam'.

### If you have already disclosed details to a potential phishing site

You should contact your bank immediately telling them when this happened and how you were contacted. This will enable your bank to investigate and help ensure that your account is protected.

### If you think your PC has been infected by spyware

You should try and remove spyware as soon as possible using anti-virus software. Alternatively you can seek help from your software or computer supplier. If you have used your online banking service prior to the attack, you should contact your bank so that they can take steps to protect your accounts from fraud. Emails you receive that you think may be part of a spyware scam can also be reported to the banking industry by visiting [www.banksafeonline.org.uk](http://www.banksafeonline.org.uk) and clicking on 'Report a scam'.

### If you think you have become involved in a money mule scam

Even if you have had nothing to do with the actual theft of funds from another person's account, by allowing your account to be used to receive and transfer such funds, you will be acting illegally. If you think you have become involved in a scam of this nature contact your bank straight away – they will advise you on what steps you should take.

## Protection for victims of fraud

Recent amendments to *The Banking Code* ensure online bankers get protection if they are a victim of fraud. The revised version of *The Banking Code* (issued in March 2008) includes a new section (12.13) that states:

"Unless you have acted fraudulently or without reasonable care you will not be liable for losses caused by someone else which take place through your online banking service".